A Novel Denial of Service Vulnerability in Long Term Evolution Cellular Networks

James Long and John D. Roth
Department of Electrical and Computer Engineering
Naval Postgraduate School
jglong, jdroth@nps.edu

Abstract

Currently many cellular networks operate using the Long Term Evolution (LTE) protocol. Therefore, most mobile subscribers interact with LTE on a daily basis, and thus are affected by the security standards and mechanisms it implements. Here, we propose a vulnerability within the LTE protocol: the mobility management control signaling, which dictates how a user equipment (UE) synchronizes with an enhanced Node-B (eNodeB) to prevent intersymbol interference. Presented are the implications and the overall effects on the bit error rate (BER) of falsified signaling which forces a UE to incorrectly advance or delay its uplink timing. Specifically, we derive a lower bound on the BER for UE that is subjected to the aforementioned signaling. Our simulation results show that a non-zero BER can be guaranteed regardless of noise conditions. Finally, we propose encryption of this signaling to prevent such an attack.

1. Introduction

Exploring and identifying Long Term Evolution (LTE) denial of service (DoS) methodologies is nothing new. In essence, the fundamental idea behind a DoS attack is to prevent a user, or users, from utilizing their device as it was designed to be used. DoS attacks are defined by two parameters: the amount of malicious traffic load generated and the impact of the attack, also known as the scope of the attack [1]. Here, traffic load can be thought of as the amount of effort required to implement the attack and scope is the number of affected users. One example of a DoS attack is classic radio jamming. Radio jamming is a deliberate use of interfering radio signals sent from one or more transmitters to garble emissions from other transmitters in order to make them unintelligible at reception [2]. In this method of DoS, the transmitted signal is subjected to artificially created noise to disrupt the signal's integrity, thereby denying the receiver an exact copy of the transmitted signal and making the received signal useless. The case of classic radio jamming can be qualified as high traffic load and high scope per the model presented by [1]. One notable aspect of radio jamming is that it usually is not used to target individual user equipment (UE). Radio jamming affects all users in a given area (i.e., high scope). Basic electromagnetic theory tells us that the closer a user is to the source of the jamming transmitter, the more affected they are by the jamming. However, in general, a malicious actor has less control over who and what they affect by employing a radio jamming DoS attack. Also, a radio jamming attack requires the affected user/users to be close to the transmitter. As soon as the affected user moves far enough away from the transmitter, they are no longer affected by the attack.

In this work we draw attention to a novel method of DoS in mobility managed networks. The proposed vulnerability leverages control signaling, normally used to ensure proper time alignment of UE uplink frames [3], in order to intentionally create misalignment. The misaligned uplink frames create intersymbol interference (ISI) and subsequently increase a UE bit error rate (BER). The traffic load requirement of this vulnerability is low, just a single packet containing falsified control signaling is required. The scope of the attack is also localized to the recipient of the falsified control signaling with minimal second-order effects. The proposed vulnerability is unique in that the physical signals themselves do not need to be overwhelmed, such as in classical jamming. Rather it takes advantage of how the protocol's structure requires devices to synchronize with a radio access point, termed enhanced Node-B (eNodeB) in the LTE protocol. Among other functions, the eNodeB is responsible for transmitting the downlink signal, and receiving the uplink signal to and from the handset (i.e., UE) [4]. This paper investigates the subject vulnerability given the current status of the LTE protocol due to its ubiquitous implementation worldwide. However, we note that the vulnerability is generally applicable to any wireless network that implements time division multiple access and mobility management.

URI: https://hdl.handle.net/10125/60188
ISBN: 978-0-9981331-2-6
(CC BY-NC-ND 4.0)

The contributions of this paper are as follows. First, we introduce the subject novel vulnerability. Second, we provide a theoretical lower bound on an affected UE's BER. Third, we leverage simulations using the Monte Carlo technique to complement the analysis and provide further insight into how a UE might be affected. Finally, we put forth a proposed amendment to the standard that would nullify the effect of this vulnerability.

The remainder of this paper is organized as follows: First, we present a review of the salient aspects of LTE. Next, we introduce the proposed vulnerability and its theoretical effects. The preceding analysis is then complemented and further illuminated by the presented simulated results. Finally, we extend the results with a discussion of their interpretation in the context of LTE-specific mechanisms such as the cyclic prefix and various modulation schemes.

2. Background

First, we will motivate the discussion by briefly discussing some fundamental technologies and theory that LTE implements. Next, we will discuss how the UE-eNodeB synchronization process works according to technical specifications as well as introducing the mechanism for mobility management. Lastly, we introduce the proposed vulnerability in detail and provide a theoretical analysis of its effect.

2.1 Mobility Management in LTE

Modern LTE architecture attempts to optimize resource efficiency by servicing as many customers as possible. In order to do that, a working group by the name of Third Generation Partnership Project (3GPP) was formed. 3GPP is the governing body of LTE standards and is responsible for issuing technical specifications. 3GPP is accountable for dictating how mechanisms such as mobility management are implemented.

LTE implements a technology referred to as orthogonal frequency division multiplexing (OFDM) where each UE is assigned a resource block corresponding to a specific frequency and time slot. Setting the frequency component aside, the width of each resource block is one millisecond [5]. Because the computers are required to work with such small units of time, they must also maintain high levels of timing accuracy in order to function properly and prevent the smearing of individual pulses (i.e., symbols) and subsequently overlaping in time (i.e., ISI) [6]. Because frames propagate at the speed of light, small changes in relative distance from one another can have significant

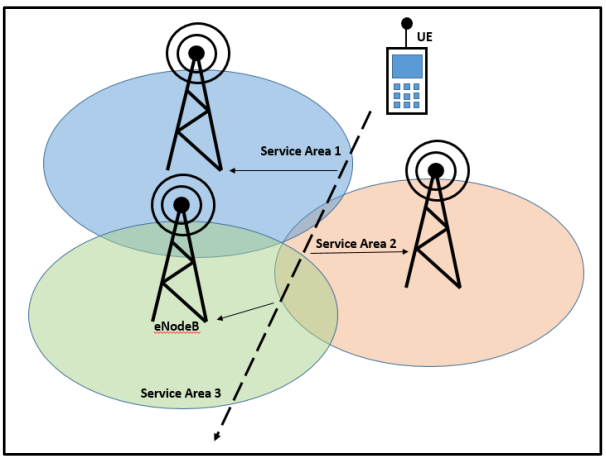

Figure 1: The UE is handed over between each eNodeB as it enters and exits new service areas.

impacts on the UE-eNodeB synchronization and the amount of induced ISI.

The designation given to the UE-eNodeB synchronization process is random access, in which a UE can request to connect to the network at any time, thus the use of the terminology *random* [3]. The necessity for UE to be synchronized with an eNodeB is driven by the need for UE to be mobile. As the UE moves around, it is handed off from one eNodeB to another as observed in Figure 1. Due to the movement of the UE, the transmitted symbols take different amounts of time to get from the UE to the eNodeB. The time it takes for a bit to traverse the distance from the UE to the eNodeB depends on the relative distance between the two. For example, in Figure 1 we can see that the UE remains mostly on the fringe of service area 1, however by the time it reaches service area 3, it is much closer to the eNodeB as demonstrated by the shorter arrow length extending from the transmission path to the eNodeB. Because the distance between the transmission path and the eNodeB changes, so too will the time it takes for the uplink frame to reach the eNodeB.

This time-domain synchronization is managed by a specific command element in the control signaling called the timing advance (TA). In order for the UE to acquire its initial TA command, it must undergo the random-access process as specified in [3] and summarized in [4]. First, the UE transmits (uplink) a random-access preamble that allows the eNodeB to approximate the UE timing. Second, based on step 1, the eNodeB issues a TA to the UE to better adjust the UE timing. Additionally, the eNodeB assigns time and frequency resources to the UE. Third, the UE requests to connect to the network. Last, if necessary, the eNodeB will resolve any contention between two UE

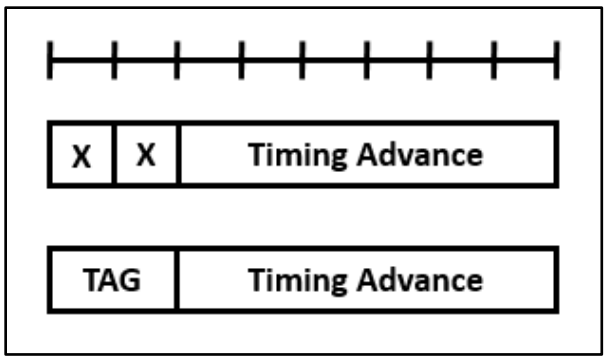

Figure 2: Legacy TA command (top) and release 10+ TA (bottom) [3].

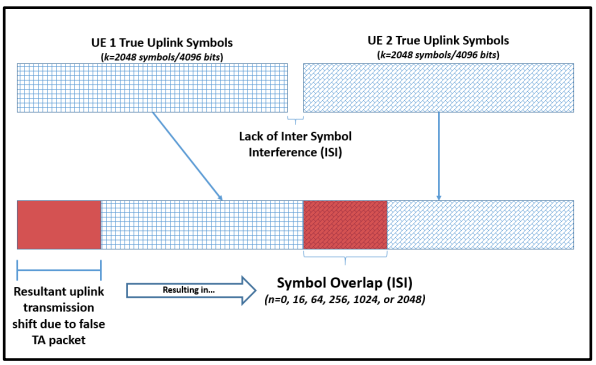

Figure 3: True Uplink Symbols and the effect of tampering with the Timing Advance mechanism.

trying to access the same time-frequency resource. Otherwise, the eNodeB will grant the UE access to the network.

Now that the UE is connected to the network, it must maintain synchronization with the servicing eNodeB to ensure that its uplink frames are arriving when the eNodeB is expecting them. The official purpose of the TA is to control advancing or delaying the uplink transmission timing to the UE [7]. Recall that our UE is assigned a specific time slot in the resource block while the other time slots in the resource block are assigned to other UEs. Therefore, if transmissions are sent at the wrong time, they will start to interfere with other frames. In this case, the frames are out of alignment causing ISI. Additionally, other users with neighboring frames are also affected by this misalignment. To rectify this issue, the eNodeB transmits a TA command to the UE, telling it when to transmit its frames so that they arrive in the designated time slot in which the eNodeB expects to receive them.

Before the structure of the TA is discussed, it is important to know that the basic unit of time in LTE is $T_s \approx .33$ nanoseconds [8]. The most frequent form of the TA is a series of eight bits: the first two of which are used to identify the TA group (TAG), and the last six correspond to values 0 to 63 as seen in Figure 2. Each bit represents one unit of time T_s. Using this series of bits, the UE is told when to transmit its uplink signal. The actual increment of time the TA represents is dependent upon the previous timing adjustment, $N_{TA,old}$. By normalizing $N_{TA,old}$ to zero, the present timing adjustment, $N_{TA,new}$, can vary from -.161 μsec to .137 μsec indicating delaying or advancing the uplink transmission timing, respectively [7].

The TAG mentioned above is implemented to manage the UE TA when the UE supports multiple component carriers (CC), possibly from multiple servicing cells. In other words, the UE is transmitting and/or receiving using multiple carriers simultaneously. In this case, the TA associated with each CC may need to be different depending on, for example, how many unique servicing cells there are. Thus, the TAG delineates which TA is associated with each CC. In the case of the same servicing cell, there is one TAG associated with multiple CC. On the other hand, if there are multiple servicing cells, then there will be multiple TAGs, each associating a TA to a specific servicing cell [9].

The legacy TA (used in LTE releases 8 and 9) does not make use of the first two bits, as seen in Figure 2. However, in releases 10 through 14, which are synonymous with LTE-Advanced (LTE-A), the subject bits are used to indicate the TAG. As customer resource demand continues to rise and 5G technologies such as heterogeneous networks start to phase into society, the TAG is becoming a more important factor in the overall TA [10].

2.2 Proposed Vulnerability

The proposed vulnerability intentionally induces ISI by sending a falsified TA command outlined in Figure 2. This disrupts and degrades the ability of the UE to interface with the larger network, thereby rendering the user unable to communicate.

The disruptive ISI-inducing command causes the UE to shift when it transmits its uplink frame as seen in Figure 3. The result of this shift causes symbols to interfere with one another.

Furthermore, this vulnerability is user-specific. During the aforementioned random-access procedure, the eNodeB assigns the UE a unique identifier used for signaling purposes called the Cell-Radio Network Temporary Identifier (C-RNTI) [4]. The C-RNTI can be thought of as a digital address for the UE. Because each UE in the servicing area of the eNodeB receives all downlink transmissions from the eNodeB, each UE uses its assigned C-RNTI to know which signals to pay attention to and which signals to disregard. Particularly

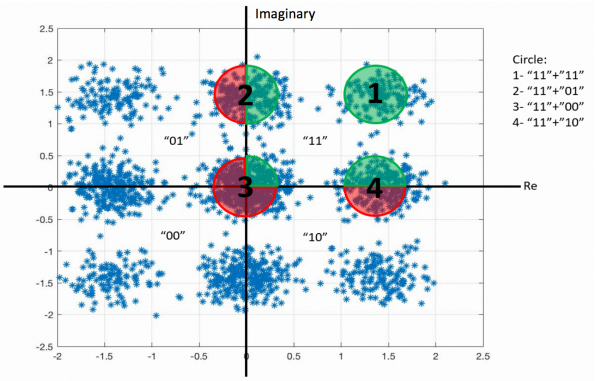

Figure 4: Visualization of ISI and its effects on error rate.

important is that the proposed DoS vulnerability requires observation of the UE's random-access procedure in order to associate the C-RNTI with the UE [10].

Since this method relies on symbols overlapping one another, the technique requires an adjacent user's symbols to overlap with. Here, the unintended, second-order effect due to induced ISI is best understood using Figure 3. Not only will the induced ISI affect an attacker's intended target, but it will also have an equal effect on the second frame.

2.3 Theoretical Degradation in high SNR Environments

To provide an analysis of the effect of the vulnerability we consider the standard additive white Gaussian noise (AWGN) channel where the received signal $r(t)$ is the original uplink signal $s(t)$ corrupted by the effects of Gaussian noise $n(t)$. That is,

$$r(t) = s(t) + n(t). \qquad (1)$$

The uplink signal is a randomly generated series of bits, modulated via quadrature phase shift keying (QPSK). QPSK modulation provides for the best-case scenario in terms of BER. By employing a QPSK scheme in our study, we give the benefit of the doubt to the BER results, while still demonstrating the potency of the vulnerability. Additionally, we are in effect bounding the lower limit of the BER. By implementing other modulation schemes, we would expect to observe even poorer BER behavior.

The AWGN is dependent upon the specified bit-energy-to-noise ratio (Eb/No). Eb/No provides a measure of the energy per bit relative to the noise floor [11].

Further, Eb/No is a normalized version of signal-to-noise ratio (SNR), which is used more often when referring to the digital environment since it allows comparison of performance across modulation schemes with different size symbol dictionaries.

To begin our derivation of a lower bound on BER consider an idealized scenario where $r(t) = s(t)$ (i.e., a noiseless channel). In this best-case scenario, the theoretical BER is zero. However, if ISI is introduced via the proposed vulnerability a minimum BER is guaranteed which depends on the magnitude of induced ISI. Utilizing Figure 4 and applying the law of total probability, we can show that for a noiseless environment the theoretical symbol error rate (SER) for a given amount of ISI is

$$SER_{Theory} = \frac{7n}{16k}, \quad \mathrm{n} \le k, \qquad (2)$$

where n is an integer number of symbols experiencing ISI and k is the total number of transmitted symbols. In Figure 4, we demonstrate the case where the original transmitted symbol is in the first quadrant ("11"). Then, another symbol is randomly generated with equal probability and subsequently added to the original transmission symbol (i.e. ISI). Through this process, we now have four possible scenarios, which are indicated by the numbered circles. The color green indicates no error, and the color red indicates a symbol error. All possible scenarios are represented by the total area in the circles, which is $\frac{16}{4}$. The area occupied in red, representing symbol error, is $\frac{7}{4}$. Now, to quantify the SER, we divide the red area (error) by the total area (all possible scenarios), and multiply by the magnitude of the symbol overlap ($\frac{n}{k}$) which results in (2). Clearly, the case where $n > k$ is not possible, hence the associated inequality. The basis of (2) is the noiseless environment where we assume that every symbol received is exactly as it was transmitted, due to the low levels of noise. Additionally, we make the assumption that the false control signaling which causes the UE to transmit early or late is properly received. This last assumption could be relaxed by including a probability of reception of the malicious packet. However, for a noiseless environment, the BER is less than or equal to one-quarter, such that

$$\lim_{n \to k} \frac{n}{4k} = \frac{1}{4}. \qquad (3)$$

Therefore, the analysis also shows that the BER is lower-bounded by (3) regardless of the actual noise level in the UE-eNodeB channel. Any further degradation of the BER will be solely a function of $n(t)$.

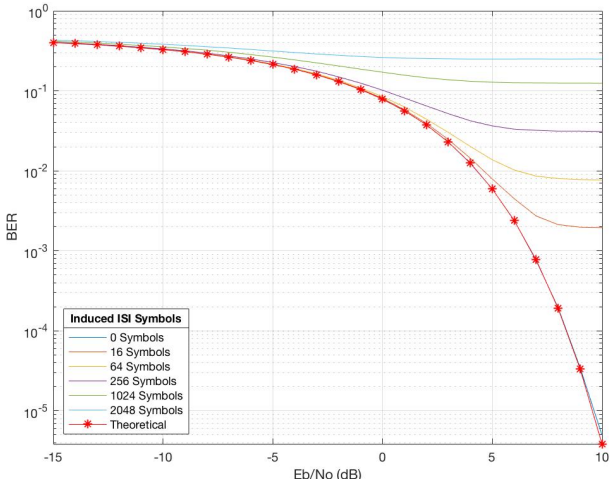

Figure 5: Bit error rate as a function of Eb/No given a specified number of ISI symbols.

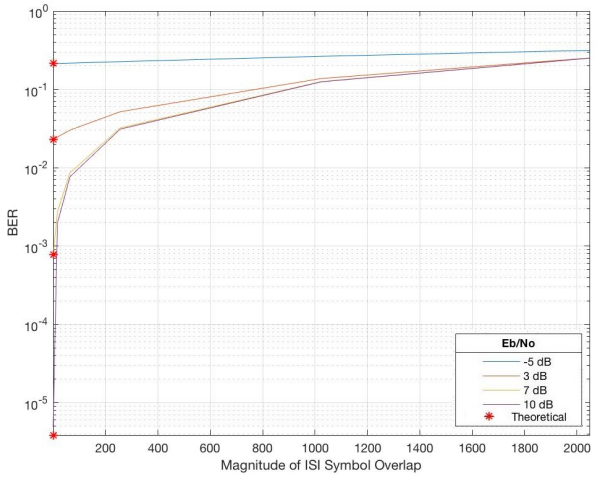

Figure 6: Bit Error Rate as a function of ISI given a specified Eb/No.

3. Simulation and Results

3.1 Simulation Environment and Parameters

ISI was modeled by randomly generating frame content and summing the first portion of the true uplink symbols with the overlapping symbols as seen in red in Figure 3. The remaining portion of the symbols is untouched. Finally, after the induced ISI all symbols were passed through (1). Implementing AWGN allowed observation of the effects on BER as a function of both ISI and noise. Finally, $r(t)$ was compared to $s(t)$, allowing calculation of the SER/BER.

During this research, we used a randomly generated frames of 4096 bits (i.e., 2048 symbols) where ones and zeros were generated with equal probability. To model the effects of modifying the signal timing, selected values of ISI, $n = [16, 64, 256, 1024, 2048]$, were chosen. Each of these values of n represents the number of frame symbols experiencing ISI. Because QPSK is used, the total frame length is 2048 symbols (i.e., 2 bits per symbol). Therefore, $n = 2048$ symbols represents the case where two frames arrive at the eNodeB simultaneously (i.e., complete ISI). For values larger than 2048 we would expect that the overall BER start to decrease since a smaller number of symbols are affected. By varying the magnitude of induced ISI, n, we were able to observe the marginal effects it has on BER. Additionally, to make the model more realistic, we included AWGN with levels between -15 dB and 10 dB in 1 dB increments.

The model does not account for coding schemes, the cyclic prefix, or use of higher-order modulation schemes. The authors plan to implement these techniques in future research in order to more accurately model the effect in modern communication schemes.

3.2 Results of the Simulation

In Figure 5, we have plotted the results of our simulation as well as the theoretical instance for zero ISI. We show the BER behavior as function of magnitude of induced ISI and Eb/No. First, note that nearly identical to the theoretical BER is the simulated case in which we did not implement any ISI. Of note, as Eb/No approaches zero, the BER performance converges to the theoretical limit of 0.5. This outcome suggests that for very noisy environments, noise is the dominant factor in BER performance. In other words, depending on the severity of noise in the channel, the presented DoS vulnerability may have little impact on BER. This low Eb/No environment is the exact outcome desired by a radio jamming DoS attack. Excluded are cases greater than 10 dB because the BER does not vary significantly with incremental changes of Eb/No for all values of ISI.

Referring to the left-hand side of Figure 5, one can see that the grouping of the BER curves is much tighter. This is due to the signal experiencing a low SNR. In this region, the true uplink transmission is affected mostly by noise, however there is a marginal effect due to the ISI at low Eb/No levels as denoted by the slight, incremental spacing between the lines. As the Eb/No value increases, the contours begin to diverge, indicating that, the BER becomes more dependent on the magnitude of the ISI.

As Eb/No continues to increase, the graphs heads-in two distinct directions. In one direction, there is no ISI, while in the other there exists ISI. In the case of zero ISI, the BER drops to zero as noise quality increases, while

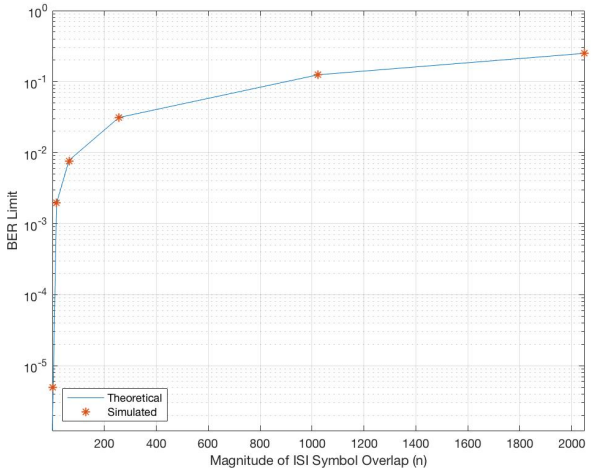

Figure 7: Bit Error Rate limit as a function of ISI for extremely low levels of noise.

for non-zero ISI values, the BER approaches non-zero values, confirming that the proposed vulnerability can guarantee a non-zero BER regardless of the channel quality.

The vulnerability makes the most significant difference in the region where Eb/No is greater than 7 dB. Here, the BER curves indicating non-zero ISI performance begins to behave asymptotically. This is due to near-perfect reception of symbols not experiencing ISI while bits being represented with symbols under ISI are being flipped with probability one-half.

Moreover, as the number of ISI symbols increases, the less effect noise has on the overall outcome of the BER as demonstrated by the relative flatness of the contours. For example, the line closest to the top of graph, indicating complete ISI (i.e., entire frame overlap), has a much flatter contour than the orange line indicating 16 ISI symbols. In cases where the noise level is undetermined, larger quantities of ISI symbols can guarantee a high BER irrespective of noise conditions. For example, given an ISI symbol magnitude of 2048, the BER at -15dB is 0.4305, and as the quality of the noise environment improves, the simulated BER approaches 0.2500 at 10 dB and greater. On the other hand, an ISI symbol count of 16 symbols yields a BER of 0.4004 at -15 dB, and as the noise environment improves the simulated BER approaches 0.0020 at 10 dB. Therefore, with high ISI little change in BER is noted over a large change in Eb/No. Alternatively, with little ISI much larger changes in BER are noted over the same large range of Eb/No. Therefore, for unknown channel conditions, high ISI guarantees the most consistent BER. These results are also shown in Figure 7, but from a different perspective. The theoretical values of BER, given no ISI are plotted in red asterisks. Selecting four values of Eb/No allows us to demonstrate

Table 1: Simulated Bit Error Rate (BER) vs. Theoretical BER.

# of ISI symbols (n)	Simulated BER (%)	Theoretical BER (%)
0	0	0
16	0.0020	0.0020
64	0.0077	0.0078
256	0.0311	0.0312
1024	0.1248	0.1250
2048	0.2500	0.2500

the dependency of BER on ISI symbols. Again, given an ISI magnitude of 2048, the BER does not vary greatly as demonstrated by the behavior of the contours on the right-hand side of the graph. However, on the left-hand side of the graph, where there is no ISI introduced, we can see the large fluctuation in BER as a result of only noise. As expected, the greater the noise, the greater the BER.

Lastly, Table 1 compares the theoretical BER from (3) to the simulated BER with values rounded to four decimal places. In every case, the simulated BER approximately equal to the theoretical BER. Recall from the analysis that we were able to bound the lower limit of the BER using (3) for a given number of ISI symbols. Thus, what the simulation provides, supports the theory. The reason for the minute discrepancy is that the simulated results are all subjected to noise, albeit in very small amounts, while the theoretical values assume no noise. Complementing Table 1, the results in Figure 7 depict the information in a graphical format to further highlight this trend. The line represents (3) above and the theoretical values from Table 1, while the red asterisks are the simulated values from Table 1. As you can see, the model very nearly reproduces the theoretical BER for each value of n. The actual simulated BER for zero ISI is $5 \cdot 10^{-6}$ which the authors approximate in Table 1 as zero.

3.3 Implications for LTE

When considering the implications of the above simulations in LTE a few key factors are noted. Perhaps most important is the lack of a cyclic prefix in the simulation. In order to reduce ISI, the current LTE standard implements a cyclic prefix to the frame structure. The cyclic prefix is used to reduce ISI caused by time dispersion as a result of multiple transmission paths [12]. Time dispersion occurs when the same signal is received starting at two different times, potentially creating a situation where the end of one frame overwrites the beginning of another frame. Therefore, the cyclic prefix replicates the end of the frame and places it at the beginning of the frame [4]. Based on the purpose of the cyclic prefix, we speculate that the effect

of ISI will be reduced and BER will drop. We suspect that there will be a minimum number of ISI symbols needed to introduce guaranteed levels of BER. Introducing any ISI less than the minimum may have little effect at all on the BER. However, more research needs to be conducted in order to quantify the outcome and effectiveness of the cyclic prefix.

Lastly, this simulation implemented a QPSK modulation scheme. Higher-order modulation schemes are used in LTE and should be considered in future work. Additionally, simulation of the physical layer can be extended to include multiplexing, specifically OFDM. OFDM is unique in that it divides a single channel into many subchannels so that multiple symbols are transmitted in parallel [13].

4. Conclusion

This paper has proposed an innovative DoS technique that simulations show would effectively generate user-specific ISI, with minimal second-order effects. Specifically, we have evaluated the current LTE mobility management climate and demonstrated within it, a flaw, which is susceptible to exploitation. Due to its lack of security, the TA mechanism that is intended to shield against ISI, actually makes it possible to create intentional uplink signal interference. Additionally, we've shown what the effects on the BER would be under these circumstances. Furthermore, we've demonstrated the ability of an assured non-zero BER given any amount of environmental noise. Most importantly, this deficiency extends beyond LTE and into the wider scope of technologies implementing unencrypted time division multiple access control. Here, we've only demonstrated the effects on a narrow portion of the overall picture.

We submit that relevant governing bodies, such as 3GPP, consider encryption of such signaling. Doing so would prevent a would-be attacker from crafting a falsified TA, thereby nullifying this vulnerability.

References

[1] R. Piqueras Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Atlantic City, NJ, 2013, pp. 1-9.

[2] Whitton J.B., and A. Larson, Propaganda towards disarmament in the war of words. Oceana Publications; 1963.

[3] 3GPP TS 36.321, release 15, (v15.1.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification," Mar. 2018.

[4] Dahlman, E., S. Parkvall, and J. Sköld, 4G LTE/LTE-Advanced for Mobile Broadband, Elsevier Ltd., 2011, Burlington, MA.

[5] 3GPP TS 36.201, release 15, (v15.0.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; General description," Mar. 2018.

[6] A. V. Oppenheim, A. S. Willsky, and S. H. Nawab, Signals &Amp; Systems (2nd Ed.), Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1996.

[7] 3GPP TS 36.213, release 15, (v15.1.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures," Mar. 2018.

[8] 3GPP TS 36.211, release 15, (v15.1.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical channels and modulation," Mar. 2018.

[9] 3GPP TS 36.300, release 15, (v15.2.0), "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall Description; Stage 2," Jun. 2018.

[10] J. Roth, M. Tummula, and J. Scrofani, "Cellular Synchronization Assisted Refinement (CeSAR): A Method for Accurate Geolocation in LTE-A Networks," System Sciences (HICSS), 2016 49th Hawaii International Conference on. IEEE, 2016.

[11] Sklar, B. Digital Communications: Fundamentals and Applications. Prentice-Hall, Inc., Upper Saddle River, NJ, USA. 1988.

[12] Larmo, A., Lindström, M., Meyer, M., Pelletier, G., Torsner, J. and Wiemann, H., "The LTE link-layer design." IEEE Communications magazine, IEEE, 2009.

[13] Hanzo, L., J. Akhtman, L. Wang, and M. Jiang, MIMO-OFDM for LTE, Wi-Fi, and WiMAX: Coherent versus Non-coherent and Cooperative Turbo-transceivers, IEEE Wiley, Hoboken, N.J., 2011.